## AMENDMENTS TO THE CLAIMS

25. (Currently Amended) A memory device comprising:

a main memory array;

an internal processor to execute programming code;

a hidden storage area coupled with the main memory array, wherein the programming code prevents access to the hidden storage area if a password is invalid; and

a bad password counter coupled with the internal processor to maintain a record of one or more invalid passwords, wherein if the bad password counter reaches a predetermined maximum value the internal processor stops processing password verification commands.

26. (Previously Presented) The memory device of claim 25, wherein the main memory array comprises a non-volatile writable memory array.

27. (Previously Presented) The memory device of claim 26, wherein the non-volatile writable memory array one or more of the following: a flash memory array, a battery backed memory array, and a polymer memory array.

28. (Original) The memory device of claim 25, wherein the hidden storage area comprises one or more hidden memory banks.

29. (Original) The memory device of claim 28, wherein the hidden memory are divided into one or more user spaces and a password space containing one or more stored valid reference passwords.

30. (Previously Presented) The memory device of claim 29, wherein the valid password allows accesses to one of the user spaces.

31. (Original) The memory device of claim 28, wherein the hidden memory banks include a swap space to copy data between the hidden memory banks without exposing the data in the hidden memory banks.

32. (Original) The memory device of claim 28, wherein the hidden storage area further comprises a bank selector to select a hidden memory bank.

33. (Original) The memory device of claim 28, wherein the hidden storage area further comprises an output bus gate to prevent access to the hidden memory banks.

34. (Original) The memory device of claim 33, wherein the hidden storage area further comprises an address decoder to open the output bus gate when provided the valid password.

35. (Previously Presented) The memory device of claim 33, wherein the hidden storage further comprises an address decoder to open the output bus gate when a valid memory address within the hidden memory banks is provided.

36. (Original) The memory device of claim 35, wherein the valid memory address is provided by a host.

Claims 37-39 (Cancelled)

40. (Currently Amended) A method, comprising:

storing one or more valid passwords in a hidden memory area;

receiving a password at an internal processor coupled with the hidden memory area;

executing programming code to verify the password against a valid reference password stored within the hidden memory area; and

maintaining a record of one or more invalid passwords at a bad password counter coupled with the internal processor, wherein if the bad password counter reaches a predetermined maximum value the internal processor stops processing password verification commands.

41. (Original) The method of claim 40, further comprising permitting access to read from the hidden memory area if the password is verified.

42. (Original) The method of claim 40, further comprising permitting access to write to the hidden memory area if the password is verified.

43. (Original) The method of claim 40, further comprising permitting access to write to the hidden memory are if a valid address in the hidden memory area is provided.

44. (Original) The method of claim 40, further comprising dividing the hidden memory area into one or more user spaces, a password space, and a swap space.

45. (Original) The method of claim 40, further comprising writing a recovery password that allows a bad password counter to be reset.

46. (Original) The method of claim 40, further comprising writing a system administrator password that allows hidden memory area contents to be reset.

47. (Original) The method of claim 40, further comprising writing a system administrator password that allows a recovery password to be reset.

48. (Original) The method of claim 40, further comprising writing a system administrator password that allows a bad password counter to be reset.

49. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

store one or more valid passwords in a hidden memory area;

receive a password at an internal processor connected to the hidden memory area;

execute programming code to verify the password against a valid reference password stored within the hidden memory area; and

maintain a record of one or more invalid passwords at a bad password counter coupled with the internal processor, wherein if the bad password counter reaches a predetermined maximum value the internal processor stops processing password verification commands.

50. (Previously Presented) The machine-readable medium of claim 49,wherein the sets of instructions which, when executed by the machine, further cause the machine to read from the hidden memory area if the password is verified.

51. (Previously Presented) The machine-readable medium of claim 49,wherein the sets of instructions which, when executed by the machine, further cause the machine to write to the hidden memory are if the password is verified and a valid address in the hidden memory is provided.

52. (Previously Presented) The machine-readable medium of claim 49, wherein the sets of instructions which, when executed by the machine, further cause the machine to divide the hidden memory area into one or more user spaces, a password space, and a swap space.

53. (Cancelled)

54. (Previously Presented) The machine-readable medium of claim 49,wherein the sets of instructions which, when executed by the machine, further cause the machine to write a system administrator password that allows hidden memory area content to be reset.

55. (Previously Presented) The medium of claim 49, wherein the sets of instructions which, when executed by the machine, further cause the machine to write a system administrator password that allows a recovery password to be reset.

56. (Cancelled)

57. (Currently Amended) A system comprising:

a wireless communication transceiver; and

a memory device coupled ~~to~~ with the wireless communications transceiver, the memory device including

a main memory array,

an internal processor to execute programming code,

a hidden storage area connected to the main memory array, wherein the programming code prevents access to the hidden storage are without a valid password, and

a bad password counter coupled with the internal processor to maintain a record of one or more invalid passwords, wherein if the bad password counter reaches a predetermined maximum value the internal processor stops processing password verification commands.

58. (Previously Presented) The system of claim 57, wherein the main memory array comprises a non-volatile writable memory array.

59. (Previously Presented) The system of claim 58, wherein the non-volatile writable memory array comprises one or more of the following: a flash memory array, a battery backed memory array, and a polymer memory array.

60. (Previously Presented) The system of claim 57, wherein the hidden storage area comprises one or more hidden memory banks.